

mobile application security system 50 for preventing hostile hosts from transmitting code to other hosts in accordance with the invention. In particular, the mobile application 40 is received from another host by a trusted host (Host n) and then later dispatched to another host to continue the execution of the mobile application 40. In this example, Host n is trusted in that the server 52 knows that the particular host will not perform nefarious acts using the mobile application 40. Therefore, the mobile application 40 dispatched from Host n is sent to the server 52 in accordance with the invention and the server 52 may perform several security measures. For example, the server 52 may receive the code of the mobile application 40 and store a copy of it in the database 62. No comparison is necessary since the host is trusted. The server 52 may then forward the mobile application 40 onto the next host, Host n+1 in this example. The mobile application 40 may then be received by and executed by Host n+1. When the mobile application 40 requires the code for execution, the known safe version of the code may be supplied to Host n+1 by the server 52 or, if the originating host is trusted, the code may be provided by the originating host. Now, a third embodiment of the mobile application security system will be described.

Please replace the paragraph beginning at page 22, line ⁴14 with the following amended paragraph:

Figure 12 is a diagram illustrating a third embodiment of the mobile application security system 50 for detecting unwanted changes to the state of a mobile application in accordance with the invention. In general, the server 52 may compare the state of the mobile application on the previous jump with the state of the mobile application on the current jump. This allows the server to detect the unwanted changes in the state of the mobile application. In more detail, a host, Host1 in this example, may create a mobile application 40 that is then dispatched to other hosts for further execution. When the mobile application 40 is dispatched, it is sent to the server 52 which may save a copy of the mobile application's state (e.g., in storage 62). The server 52 may then forward the mobile application 40 to the next host, Host2 in this example. Host2 may receive the mobile application 40, execute it and then forward it onto the next host. The server 52 may receive the mobile application 40 from the next host and compare the state of the mobile

application 40 received from the next host to the state of the mobile application 40 saved in the database to determine if changes have occurred. If the comparison does not detect any unwanted changes with the mobile application 40, the server 52 may forward the mobile application 40 onto the next host. Thus, in this embodiment, a host that executes the mobile application 40 is unable to insert changes into the mobile application's state since those changes will be identified by the server 52 when the comparison step is executed by the server 52. Now, a fourth embodiment of the mobile application security system will be described.

WLF 7-13-07 Please replace the paragraph beginning at page 23, line ¹⁹~~16~~ with the following amended paragraph:

Figure 13 is a diagram illustrating a first example of a fourth embodiment of the mobile application security system 50 for detecting unwanted changes in the itinerary of the mobile application in accordance with the invention. In general, on each jump of the mobile application, the server may determine the host from which the mobile application was dispatched and the hosts to which the mobile application is dispatched. In particular, this permits the server 52 to enforce the itinerary (e.g., the hosts where the mobile application is going to be executed) of the mobile application. In more detail, a first host (Host1) may create a mobile application 40 and then may dispatch the mobile application 40 to another host through the server 52 in accordance with the invention. When the server 52 receives the mobile application 40, the server 52 may store a copy of the itinerary of the mobile application 40 in the database 62. The server 52 may then forward the mobile application 40 to the next host (Host2) according to the itinerary. Now, another example of the embodiment for detecting changes in the itinerary will be described.

WLF 7-13-07 Please replace the paragraph beginning at page 24, line ¹¹~~7~~ with the following amended paragraph:

Figure 14 is a diagram illustrating a second example of a fourth embodiment of the mobile application security system 50 for detecting unwanted changes in the itinerary of the mobile application in accordance with the invention wherein the itinerary of a mobile application is already stored in the server. In more detail, a first host (Host n) may dispatch a mobile

application 40 to another host through the server 52 in accordance with the invention. When the server 52 receives the mobile application 40, the server 52 may compare the current itinerary of the mobile application 40 to a stored copy of the itinerary to ensure they match each other. If the itineraries match, then the server 52 may forward the mobile application 40 onto the next host (Host n+1) that receives the mobile application 40 and executes it. Now, another example of the embodiment for detecting changes in the itinerary will be described.

WP 7-13-07 Please replace the paragraph beginning at page ²⁵~~24~~, line ¹~~17~~ with the following amended paragraph:

Figure 15 is a diagram illustrating a third example of a fourth embodiment of the mobile application security system 50 for detecting unwanted changes in the itinerary of the mobile application in accordance with the invention wherein the itinerary may be changed. In more detail, a first host (Host n) which has received a mobile application 40 from another host may dispatch the mobile application 40. The mobile application 40 then passes through the server 52 in accordance with the invention. When the server 52 receives the mobile application 40 in accordance with the invention, it may ensure that the historical portion of the itinerary is accurate by comparing the previously saved itinerary with the new itinerary. If the historical portion of the itinerary is accurate, the server 52 forwards the mobile application 40 to the next host (Host n+1). Now, a fifth embodiment of the mobile application security system will be described.

WP 7-13-07 Please replace the paragraph beginning at page 25, line ¹¹~~6~~ with the following amended paragraph:

Figure 16 is a diagram illustrating a first example of a fifth embodiment of the mobile application security system 50 for preventing untrusted hosts from launching a mobile application in accordance with the invention. In general, on each jump of the mobile application, the server may determine if the mobile application has previously been in the system. For example, if the host from which the mobile application is sent is an untrusted host, the server may prevent the mobile application from being forwarded to the next host. In more detail, as shown in Figure 16, a first host (Host1) may create a mobile application 40 and then later

dispatch it to another host. In accordance with the invention, the dispatched mobile application 40 first is sent to the server 52. The server 52 may determine that the mobile application 40 is new and therefore further investigation is necessary. If the server 52 then determines that the particular host is allowed (e.g., is trusted to) to launch mobile applications, the server 52 may forward the mobile application 40 to the next host (Host2) so that Host2 receives the mobile application 40.

WP 7.13.07 Please replace the paragraph beginning at page ²⁶~~25~~, line ³~~18~~ with the following amended paragraph:

Figure 17 is a diagram illustrating a second example of a fifth embodiment of the mobile application security system 50 for preventing untrusted hosts from launching a mobile application in accordance with the invention. In particular, an untrusted host (Host1) may create a new mobile application 40 that is then later dispatched. The mobile application 40 is then sent dispatched to the server 52 first in accordance with the invention. The server 52 determines that the host dispatching the mobile application 40 is untrusted so that the server 52 does not forward the mobile application 40 to the next host.

WP 7.13.07 Please replace the paragraph beginning at page 26, line ¹⁰~~4~~ with the following amended paragraph:

Figure 18 is a diagram illustrating a third example of a fifth embodiment of the mobile application security system 50 for preventing untrusted hosts from launching a mobile application in accordance with the invention wherein a subsequent dispatch of the mobile application occurs. In particular, a host (Host n) attempts to dispatch a mobile application 40 to another host which must pass through the server 52 in accordance with the invention. When the mobile application 40 is received by the server 52, the server 52 may determine that the mobile application 40 is not new (e.g., the server 52 knows about the mobile application 40 and knows that it is safe) and forwards the mobile application 40 to the next host (Host n+1). Now, a summary of how the above procedures raise the security level of a mobile application environment will be described.